UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,319	06/12/2001	Mark Crosbie	10004512-1	2127

7590 10/18/2004

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80528-9599

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/878,319	CROSBIE ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 10/11/2001. Claims 1 – 48 were received for consideration. No preliminary amendments were filed. Claims 1 – 48 are currently being considered.

Claim Objections

2. Claims 31and 35 are objected to because of the following informalities:

Claim 31 recites "director,". Replace with "directory".

Claim 35 recites "vmunix,". Replace with "vmunix".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1- 48 are rejected under 35 U.S.C. 102(e) as being anticipated by Moran (U.S. Patent Number 6,647,400).

Regarding Claim 1, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

reading kernel records (Column 7 line 39 – Column 8 line 20 and Column 11 lines 15 – 54);

reformatting each of the read kernel records into a different format (Column 9 line 54 – Column 10 line 32);

parsing the records and comparing the parsed records against one or more templates (Column 18 lines 6 – 58).

Regarding Claim 29, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

monitoring a predetermined set of files for modifications (Column 8 lines 6 – Column 10 line 55 and Column 11 lines 16 – 54);

monitoring a predetermined set of directories for modifications (Column 8 line 6 – Column 10 line 55 and Column 11 lines 16 – 54);

generating an alert for each occurrence of a modification of a monitored file (Column 10 lines 14 – 55; Column 13 lines 1 – 31 and Column 35 lines 9 – 42); and

generating an alert for each occurrence of a modification of a monitored directory (Column 10 lines 14 – 55; Column 13 lines 1 – 31 and Column 35 lines 9 – 42).

Regarding Claim 44, Moran teaches and describes a method of detecting changes to log files (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

monitoring a user defined list of files for attempts to modify any of the files in any way other than appending (Column 12 line 6 – 67).

Regarding Claim 46, Moran teaches and describes a method of detecting intrusions (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

monitoring repeated failed login attempts (Column 19 line 49 - Column 20 line 67); and

generating an alert if a predetermined threshold is exceeded (Column 8 lines 6 – 46; Column 19 line 49 – Column 20 line 67 and Column 21 lines 1 – 63).

Regarding Claim 47, Moran teaches and describes a method of detecting race condition attack (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

monitoring file accesses that a privileged program performs (Column 12 lines 6 – 67 and Column 20 lines 36 - 67)

generating an alert if an inode for a file reference appears to have unexpectedly changed (Column 8 lines 6 – 46; Column 19 line 49 – Column 20 line 67; Column 23 lines 14 – 46 and Column 27 lines 32 – 36).

Claim 2 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the kernel audit logs includes information about each system call (Column 8 line 6 – 46 and Column 9 lines 12 – 65).

Claim 4 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising monitoring system log files (Column 10 lines 14 – 55).

Claim 5 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising a system call (Column 10 lines 33 – 47).

Claim 6 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the system call was initiated by a library call (Column 10 lines 33 – 47 and Column 13 lines 1 – 11).

Claim 8 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising determining that an intrusion has occurred and generating an alert message (Column 8 lines 6 – 46).

Claim 9 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising encrypting information sent between the host-based intrusion system and a network (Column 16 lines 15 – 29).

Claim 10 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising displaying an alert message that an intrusion has occurred (Column 8 lines 6 – 46 and Column 10 lines 14 – 55).

Claim 11 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the

different format is a memory mapped file (Column 9 line 54 – Column 10 line 32 and Column 22 line 65 – Column 23 line 3);

Claim 14 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a modification of files/directories template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40).

Claim 15 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a change to log files template (Column 2 lines 40 – 47; Column 10 lines 14 – 55 and Column 11 lines 41 – 54).

Claim 16 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a SetUID files template (Column 9 lines 33 – 47 and Column 12 lines 46 – 67).

Claim 17 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a creation of world-writables template (Column 11 line 55 – Column 12 line 67).

Claim 18 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a repeated failed logins template (Column 19 line 49 – Column 20 line 67).

Claim 19 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a repeated failed SU commands template (Column 23 lines 14 – 46 and Column 25 lines 15 – 45).

Claim 20 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a race conditions attack template (Column 12 lines 31 – 67).

Claim 21 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a buffer overflow attacks template (Column 9 lines 33 – 47 and Column 33 line 64 – Column 34 line 42).

Claim 22 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is a modification of another user's file template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40).

Claim 23 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein one or more templates is a monitor for the start of interactive sessions template (Column 38 lines 31 – 51).

Claim 24 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the

one or more template is a monitor logins/logouts template (Column 23 lines 14 – 46 and Column 24 lines 33 – 41).

Claim 25 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is chosen from the group including:

a modification of files/directories template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40);

a change to log files template (Column 2 lines 40 – 47; Column 10 lines 14 – 55 and Column 11 lines 41 – 54);

a SetUID files template (Column 9 lines 33 – 47 and Column 12 lines 46 – 67);

a creation of world-writables template (Column 11 line 55 – Column 12 line 67);

a repeated failed logins template (Column 19 line 49 – Column 20 line 67);

a repeated failed SU commands template (Column 23 lines 14 – 46 and Column 25 lines 15 – 45);

a race conditions attack template (Column 12 lines 31 – 67);

a buffer overflow attacks template (Column 9 lines 33 – 47 and Column 33 line 64 – Column 34 line 42);

a modification of another user's file template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40);

a monitor for the start of interactive sessions template (Column 38 lines 31 – 51); and

a monitor logins/logouts template (Column 23 lines 14 – 46 and Column 24 lines 33 – 41).

Claim 26 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the kernel records are read from different computers (Column 10 lines 14 – 55 and Column 17 line 50 – Column 18 line 5).

Claim 27 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein parsed records are compared against the one or more templates using at least one correlator (Column 11 lines 16 – 28; Column 23 lines 14 – 46 and Column 24 lines 47 – 51).

Claim 28 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein

said parsing step compares the parsed records against one or more templates simultaneously (Column 32 line 44 – Column 33 line 11).

Claim 30 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

determining which files to monitor of all files on a computer to form the predetermined set of files; determining which directories to monitor of all directories on a computer to form the predetermined set of directories (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

Claim 31 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising, for each said determining step, specifically including a file or directory, specifically excluding a file or directory or not specifically including or excluding a file or directory (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

Claim 32 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2

– 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein a file or directory which is not specifically included or excluded is monitored (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

Claim 33 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein if a directory is specifically excluded and a file in the specifically excluded file is specifically included then the file is monitored (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

Claim 34 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes a system kernel file and system kernel configuration files (Column 8 lines 6 – 46; Column 11 line 16 – Column 12 line 30; Column 23 lines 14 – 46 and Column 32 line 44 – Column 33 line 62).

Claim 35 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the

predetermined set of files includes /stand/vmunix, /stand/kernel and stand/bootconf (Column 32 line 44 – Column 33 line 62).

Claim 36 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files defining the users on a system and files used to create accounts (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 25 line 15 – Column 26 line 45).

Claim 37 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes /etc/passwd and /etc/group (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 32 line 49 – Column 33 line 11).

Claim 38 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files which control what network services are running

and which controls programs used to fulfill service requests (Column 19 lines 28 – 65 and Column 21 line 1 – 14).

Claim 39 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes /etc/inetd.conf (Column 11 line 55 – Column 12 line 30; Column 20 lines 36 – 67 and Column 32 line 49 – Column 33 line 11).

Claim 40 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes files which are used to control the remote access of the user root without requiring a password (Column 23 lines 14 – 46 and Column 35 lines 9 – 63).

Claim 41 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of files includes/.rhosts and /.shosts (Column 9 lines 1 – 22 and Column 35 lines 9 – 63).

Claim 42 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the set of files specifically excluded includes temporary files created by a program view (Column 27 line 32 – Column 29 line 52).

Claim 43 is rejected as applied above in rejecting Claim 29. Furthermore, Moran teaches and describes a method of detecting changes to critical files/directories (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the predetermined set of directories includes Jbin, /sbin and /usr/bin (Column 36 line 7 – Column 37 line 7 and Column 39 lines 43 – 65).

Claim 45 is rejected as applied above in rejecting Claim 44. Furthermore, Moran teaches and describes a method of detecting changes to log files (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the user defined list includes: /var/adm/utmp /var/adm/btmp var/adm/wtmp /etc/utmp /etc/btmp /etc/wtmp (Column 19 line 66 – Column 20 line 5 and Column 23 lines 35 – Column 24 line 67).

Claim 48 is rejected as applied above in rejecting Claim 47. Furthermore, Moran teaches and describes a method wherein a list of users being monitored

includes root, daemon, bin, sys, adm, uucp, lp, nuucp. (Column 19 line 66 – Column 20 line 5; Column 22 lines 65 – Column 24 line 67; Column 36 line 7 – Column 37 line 7 and Column 39 lines 43 – 65).

Claim 3 is rejected as applied above in rejecting Claim 2. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the kernel audit logs includes information about each system call (Column 8 line 6 – 46 and Column 9 lines 12 – 47).

Claim 13 is rejected as applied above in rejecting Claim 2. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising converting the kernel records into an ASCII format for comparison against the one or more templates (Column 10 lines 14 – 53; Column 11 lines 29 – 40 and Column 13 lines 26 – 31).

Claim 7 is rejected as applied above in rejecting Claim 3. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising storing each system call in a circular buffer (Column 8 line 6 – 46; Column 9 lines 12 – 47).

Claim 12 is rejected as applied above in rejecting Claim 4. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising converting the system log files into an ASCII format for comparison against the one or more templates (Column 9 line 54 – Column 10 line 32).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Schoffelman et al. (U.S. Patent Number: 6,119,170) Method and Apparatus for TCP/IP multihoming on a host system configured with multiple independent transport provider system.

Williams (U.S. Patent Number: 6,304,973) Multi-Level security network system.

5. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or faxed to:** (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
October 01, 2004.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100